

WHAT IS CLAIMED IS:

1. A method comprising:

using a grid network architecture that includes a plurality of serving computers
including using a grid manager to maintain global mappings associated with tenants and a
5 plurality of directory service instances, wherein the grid manager operates in part to
monitor a deployment status of the plurality of directory service instances and make one or
more new directory service instances available to the tenants when called, wherein the grid
manager provides global mapping information for synchronizing directory service instance
updates;

10 using the ~~creating a~~ plurality of directory service instances in part to ~~that~~ define
access privileges for groups of customers requesting services of the serving computers,
each directory service instance being independent of other directory service instances and
including one or more organizational units, wherein each organizational unit is associated
with a distinct customer and includes authorized users and one or more authorized foreign
15 principle objects (FPOs);

populating each organizational unit with customer data used to control access to
services of the serving computers; and

storing the directory service instances in computer readable storage.

2. The method of claim 1, further comprising receiving access requests for
20 access to a datacenter including using domain information of each request to identify an
organizational unit of a directory service instance corresponding to a user issuing the
request wherein each FPO includes mapping parameters that point to another user object,
group, or directory service instance of a different organizational unit.

3. The method of claim 1, further comprising using the directory service
25 instances in conjunction with a domain that includes online resources and service accounts
corresponding to dedicated service farms.

4. The method of claim 1, further comprising creating organizational units for
each directory service instance, each organizational unit to include the ~~one or more~~
authorized users, one or more authorized groups, and the one or more authorized ~~foreign~~
30 ~~principle objects (FPOs), wherein the one or more authorized FPOs include one or more~~
non-employee users with a reference to one of a partner tenant and a support agent role.

5. The method of claim 4, further comprising creating organizational units of
each data instance to include mappings between FPOs and organizational units.

6. The method of claim 5, further comprising examining a FPO of a first organizational unit as part of locating a second organizational unit to verify support access.

7. The method of claim 1, further comprising denying access to a requested service if a requesting user is not associated with an organizational unit.

8. The method of claim 1, further comprising providing access to the requested services if a requesting user is associated with an organizational unit and included in a security group having defined access permissions.

9. The method of claim 1, further comprising using a plurality of user classes as part of populating each organizational unit.

10. 8. The method of claim 1, further comprising updating directory service instances to maintain current access permissions within corresponding organizational units.

11. The method of claim 1, further comprising adding additional directory service instances to support additional customers.

12. The method of claim 1, further comprising providing real-time inventory of customer information to facilitate user authorization and resource management by building service tokens for permitted users of a grid network architecture.

13. 9. A system comprising:

server resources including processing and memory components to support one or more server farms as part of providing an online application service;

a synchronization component to synchronize online customer data with the online application service using a number of directory service instance (DSI) data

structures that include customer and partner information, wherein each DSI data structure

includes one or more organizational units, wherein each organizational unit is associated with a distinct customer and includes authorized users and one or more authorized FPOs;

a grid manager to maintain global mappings associated with tenants and the number of DSI data structures, wherein the grid manager operates in part to monitor a deployment status of the number of DSI data structures and make one or more new DSI data structures available to the tenants when called, wherein the grid manager provides global mapping information for synchronizing DSI data structure updates;

storage to store the DSI data structures; and

a claim provider component to query a domain controller associated with a DSI data structure stored in the storage to control access to the server resources.

14. The system of claim 13, wherein each DSI data structure includes a number of organizational unit data structures including user objects, group objects, and subscription objects.

15. The system of claim 14, wherein each DSI data structure includes multiple customer organizational units, each unit including customer employees, security groups, and extranet users.

16. The system of claim 14, wherein the server resources are accessible as part of an online service and based in part on at least one access type.

17. A computer readable storage device which stores encoded instructions used in part to provide online services comprising:

maintaining global mappings associated with tenants and a plurality of directory service instances;

monitoring a deployment status of the plurality of directory service instances;

making one or more new directory service instances available to the tenants when called and providing global mapping information for synchronizing directory service instance updates;

receiving a request for an online resource of a data grid network;

obtaining access information from the request;

identifying a directory service instance associated with the access information, wherein each directory service instance includes one or more organizational units, wherein each organizational unit is associated with a distinct customer and includes authorized users and one or more authorized FPOs; and

examining the directory service instance to determine if the request issued from an authorized user and an access level of the authorized user.

18. The computer readable storage device of claim 17 which stores encoded instructions to control access based in part on an associated permission of an existing user of an augmented security group.

19. The computer readable storage device of claim 17 which stores encoded instructions to control access to an online asset based in part on a subscription and user type.

20. The computer readable storage device of claim 17 which stores encoded instructions that provide online services including building a service collection token using in part the access information augmented with any group claims.